(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2000－305899
（P2000－305899A）
(43)公開日　平成12年11月２日(2000.11.2)

(51)Int.Cl.⁷	識別記号	ＦＩ		テーマコード（参考）
Ｇ０６Ｆ　15/00	３３０	Ｇ０６Ｆ　15/00	３３０Ｂ	５Ｂ０４９
17/60		15/21	３４０Ｂ	５Ｂ０８５

審査請求　未請求　請求項の数11　ＯＬ　（全 19 頁）

(21)出願番号　特願平11－113058

(22)出願日　平成11年４月21日(1999.4.21)

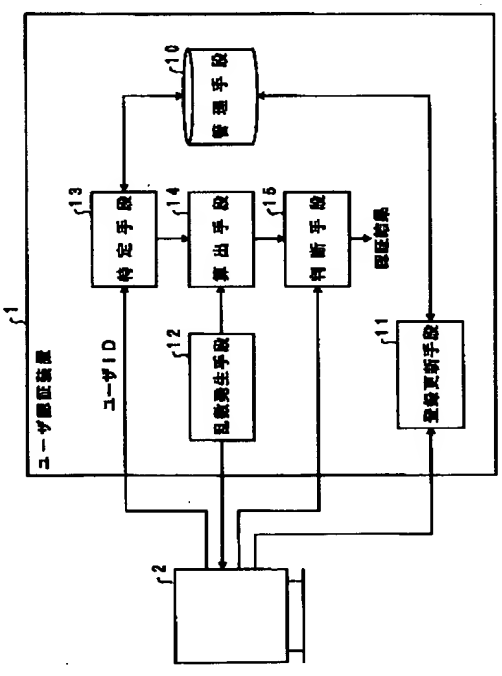
(71)出願人　000005223
富士通株式会社
神奈川県川崎市中原区上小田中４丁目１番１号
(72)発明者　佐藤　恒夫
神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内
(72)発明者　古手川　清
大分県大分市東春日町17番58号　株式会社富士通大分ソフトウェアラボラトリ内
(74)代理人　100095072
弁理士　岡田　光由　（外１名）

最終頁に続く

(54)【発明の名称】　ユーザ認証装置及び方法とユーザ認証用カードとプログラム記録媒体

(57)【要約】
【課題】本発明は、ユーザ認証に用いるユーザ認証装置に関し、ユーザやシステムに負荷をかけることなく高いセキュリティを実現することを目的とする。
【解決手段】ユーザに提示される乱数とユーザ認証対象に対応した計算式とから、ユーザ認証に用いる数値を算出する算出手段と、その乱数の提示に応答して入力されてくる数値と、算出手段の算出する数値とが一致するのか否かを判断する判断手段とを備えるように構成する。この構成に従って、ユーザの入力する数値が他人に見られてしまっても秘密性を保持でき、高いセキュリティを実現できるようになる。そして、ユーザは計算式のみを覚えれば足りるとともに、システムは計算式のみを記憶すれば足り、これにより、ユーザやシステムに負荷をかけることなく高いセキュリティを実現できるようになる。

本発明の原理構成図



1

【特許請求の範囲】

【請求項１】　ユーザ認証に用いるユーザ認証装置であって、

ユーザに提示される乱数とユーザ認証対象に対応した計算式とから、ユーザ認証に用いる数値を算出する算出手段と、

上記乱数の提示に応答して入力されてくる数値と、上記算出手段の算出する数値とが一致するのか否かを判断する判断手段とを備えることを、

特徴とするユーザ認証装置。

【請求項２】　請求項１記載のユーザ認証装置において、

算出手段は、計算式が演算子を含まない数字列である場合には、その数字列を算出結果とすることを、

特徴とするユーザ認証装置。

【請求項３】　請求項１又は２記載のユーザ認証装置において、

算出手段は、計算式がユーザ認証時に応じて変化する変数値を含む場合には、ユーザに提示する乱数とユーザ認証対象に対応した計算式と該変数値とから、ユーザ認証に用いる数値を算出することを、

特徴とするユーザ認証装置。

【請求項４】　ユーザ認証に用いるユーザ認証装置であって、

ユーザＩＤとユーザ認証対象に対応した計算式との対応関係を管理する管理手段と、

上記管理手段の管理データから、指定されるユーザＩＤに対応付けられる計算式を特定する特定手段と、

ユーザに提示される乱数と上記特定手段の特定する計算式とから、ユーザ認証に用いる数値を算出する算出手段と、

上記乱数の提示に応答して入力されてくる数値と、上記算出手段の算出する数値とが一致するのか否かを判断する判断手段とを備えることを、

特徴とするユーザ認証装置。

【請求項５】　請求項４記載のユーザ認証装置において、

ユーザから入力されてくる計算式と、管理手段に管理される該ユーザＩＤの指す計算式とが一致することを条件にして、管理手段に管理される計算式を更新する更新手段を備えることを、

特徴とするユーザ認証装置。

【請求項６】　請求項４又は５記載のユーザ認証装置において、

算出手段は、管理手段に管理される計算式が演算子を含まない数字列である場合には、その数字列を算出結果とすることを、

特徴とするユーザ認証装置。

【請求項７】　請求項４、５又は６記載のユーザ認証装置において、

2

算出手段は、管理手段に管理される計算式がユーザ認証時に応じて変化する変数値を含む場合には、ユーザに提示する乱数とユーザ認証対象に対応した計算式と該変数値とから、ユーザ認証に用いる数値を算出することを、

特徴とするユーザ認証装置。

【請求項８】　ユーザ認証に用いるユーザ認証方法であって、

ユーザに提示される乱数とユーザ認証対象に対応した計算式とから、ユーザ認証に用いる数値を算出する第１の処理過程と、

上記乱数の提示に応答して入力されてくる数値と、第１の処理過程で算出した数値とが一致するのか否かを判断する第２の処理過程とを備えることを、

特徴とするユーザ認証方法。

【請求項９】　カードの所有者の認証用に用意されるユーザ認証用カードにおいて、

ユーザＩＤを記録することに加えて、ユーザ認証対象に対応した計算式を記録するように構成されることを、

特徴とするユーザ認証用カード。

【請求項１０】　請求項９記載のユーザ認証用カードにおいて、

ユーザ認証対象に対応した計算式に代入される乱数を発生する乱数発生手段を備えることを、

特徴とするユーザ認証用カード。

【請求項１１】　ユーザ認証に用いるユーザ認証装置の実現に用いられるプログラムが格納されるプログラム記録媒体であって、

ユーザに提示される乱数とユーザ認証対象に対応した計算式とから、ユーザ認証に用いる数値を算出する算出処理と、

上記乱数の提示に応答して入力されてくる数値と、上記算出処理の算出する数値とが一致するのか否かを判断する判断処理とをコンピュータに実行させるプログラムが格納されることを、

特徴とするプログラム記録媒体。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、ユーザ認証に用いるユーザ認証装置及び方法と、カードの所有者の認証用に用意されるユーザ認証用カードと、ユーザ認証装置の実現に用いられるプログラムが格納されるプログラム記録媒体とに関し、特に、ユーザやシステムに負荷をかけることなく高いセキュリティを実現するユーザ認証装置及び方法と、ユーザやシステムに負荷をかけることなく高いセキュリティを実現するユーザ認証用カードと、そのユーザ認証装置の実現に用いられるプログラムが格納されるプログラム記録媒体とに関する。

【０００２】コンピュータ社会の発達により、様々な情報処理分野で、コンピュータを使ったユーザ認証が行われるようになってきた。このユーザ認証が誤ったり悪用

されたりすると、個人に多大な損害を及ぼすとともに、社会に大きな混乱を招くことになる。これから、高いセキュリティを実現するユーザ認証技術の構築が叫ばれている。

【０００３】

【従来の技術】最も広く用いられているユーザ認証技術としては、ユーザに４桁などで定義される暗証番号を登録させる構成を採って、ユーザ認証の必要があるときに、ユーザに自分の暗証番号を入力させ、その入力させた暗証番号と登録されている暗証番号とが一致するのか否かをチェックしていくことで、正規のユーザであるのか否かをチェックしていくという方法がある。

【０００４】しかしながら、従来技術のように、絶対的な数値で定義される絶対的な暗証番号を用いる場合、ユーザが暗証番号を入力しているときに、その暗証番号を他人に見られてしまうと、その暗証番号の秘密性がなくなることで、高いセキュリティを実現できないという問題点がある。

【０００５】更に、従来技術のように、絶対的な数値で定義される絶対的な暗証番号を用いる場合、ユーザは、暗証番号として、電話番号や生年月日や住所番号など自分に関係する覚えやすい数値を用いることが多く、これから、この従来技術に従っていると、他人に暗証番号が知られる可能性が高いことで、高いセキュリティを実現できないという問題点もある。

【０００６】このような問題点の解決を図るために、特開昭63-170764 号で、ユーザに対して、計算式と固有値とを登録させる構成を採るとともに、ユーザ認証時に時間に依存して変化する変数を発生させる構成を採って、ユーザ認証の必要があるときに、発生変数をその計算式に代入した結果がその固有値となる数値をユーザに入力させ、その入力させた数値とシステムの計算結果とが一致するのか否かをチェックしていくことで、正規のユーザであるのか否かをチェックするという技術が開示された。

【０００７】この特開昭63-170764 号で開示されたユーザ認証技術では、例えば、ユーザは、予め計算式「ｘ＋ｙ」と固有値「z_0 ＝７」とを登録しておき、時間に依存して変化する変数ｘの値として「３」が表示されるときには、「ｘ＋ｙ＝７」を実現する「ｙ＝４」を入力していくことで、本人であることを入力できるようになる。

【０００８】

【発明が解決しようとする課題】確かに、特開昭63-170764 号で開示されたユーザ認証技術に従うと、ユーザは、暗証番号のような固定の数値を入力する訳ではないので、入力する数値が他人に見られてしまっても秘密性を保持でき、高いセキュリティを実現できるというメリットが得られる。

【０００９】しかしながら、この特開昭63-170764 号で開示されたユーザ認証技術に従うと、ユーザは、自分の登録した計算式と固有値との両方を覚えていなければならないとともに、固有値から逆算していくという暗算を行わなければならず、大きな負荷を強いられるという問題点がある。

【００１０】更に、システムは、ユーザの登録した計算式と固有値との両方をメモリに記憶しなければならず、大きなメモリ容量を強いられるという問題点がある。

【００１１】本発明はかかる事情に鑑みてなされたものであって、ユーザやシステムに負荷をかけることなく高いセキュリティを実現する新たなユーザ認証装置及び方法の提供と、ユーザやシステムに負荷をかけることなく高いセキュリティを実現する新たなユーザ認証用カードの提供と、そのユーザ認証装置の実現に用いられるプログラムが格納される新たなプログラム記録媒体の提供とを目的とする。

【００１２】

【課題を解決するための手段】図１に本発明の原理構成を図示する。

【００１３】図中、１は本発明を具備するユーザ認証装置であって、ユーザ認証処理を実行するもの、２はユーザ認証装置１の備える端末であって、ユーザとの対話手段となるものである。

【００１４】本発明のユーザ認証装置１は、管理手段１０と、登録更新手段１１と、乱数発生手段１２と、特定手段１３と、算出手段１４と、判断手段１５とを備える。

【００１５】この管理手段１０は、ユーザＩＤとユーザ認証対象に対応した計算式（単なる数字列のこともある）との対応関係を管理する。登録更新手段１１は、ユーザと対話することで、管理手段１０に計算式を登録したり、管理手段１０に登録される計算式を更新する。乱数発生手段１２は、規定の数の数字列からなる乱数（１つの数字のこともある）を発生してユーザに提示する。

【００１６】特定手段１３は、管理手段１０の管理データから、指定されるユーザＩＤに対応付けられる計算式を特定する。算出手段１４は、乱数発生手段１２の発生する乱数と特定手段１３の特定する計算式とから、ユーザ認証に用いる数値を算出する。判断手段１５は、乱数発生手段１２の提示する乱数に応答して入力されてくる数値と、算出手段１４の算出する数値とが一致するのか否かを判断することでユーザ認証を実行する。

【００１７】ここで、本発明のユーザ認証装置１の持つ機能は具体的にはプログラムで実現されるものであり、このプログラムは、フロッピィディスクなどに格納されたり、サーバなどのディスクなどに格納され、それらからユーザ認証装置１にインストールされてメモリ上で動作することで、本発明を実現することになる。

【００１８】このように構成される本発明のユーザ認証装置１では、登録更新手段１１は、端末２から入力され

てくる計算式（単なる数字列のこともある）を受け取り、ユーザＩＤとの対応を取りつつ、その計算式を管理手段１０に登録することで、管理手段１０に対して、ユーザＩＤとユーザ認証対象に対応した計算式との対応関係を登録する。そして、管理手段１０に登録した計算式の更新要求があるときには、端末２から、その計算式と一致する計算式が入力されてくることを条件にして、その計算式に代わる新たな計算式を受け取り、それに従って管理手段１０に登録した計算式を更新する。

【００１９】このようにして、登録更新手段１１の処理に従って、管理手段１０に、ユーザＩＤとユーザ認証対象に対応した計算式（単なる数字列のこともある）との対応関係が管理されることになる。

【００２０】この管理手段１０の管理データを受けて、ユーザＩＤを指定してユーザ認証の要求が発行されると、特定手段１３は、管理手段１０の管理データから、そのユーザＩＤに対応付けられる計算式を特定する。一方、乱数発生手段１２は、乱数を発生して、端末２のディスプレイ画面に表示するとともに、その発生した乱数を算出手段１４に通知する。

【００２１】これを受けて、算出手段１４は、乱数発生手段１２の発生した乱数と特定手段１３の特定した計算式とから、ユーザ認証に用いる数値を算出する。そして、判断手段１５は、乱数発生手段１２の提示した乱数に応答して端末２からの入力されてくる数値と、算出手段１４の算出した数値とが一致するのか否かを判断することでユーザ認証を実行する。

【００２２】このときに、算出手段１４は、計算式として演算子を含まない数字列が特定される場合には、その数字列を算出結果としていくことで、従来から用いられている数字列の暗証番号の利用を可能にする。

【００２３】また、算出手段１４は、計算式がユーザ認証時に応じて変化する変数値（例えば、ユーザ認証時が１月～１２月のときに、それらの月のそれぞれに数字“１”～“１２”を割り付けるような場合）を含む場合には、乱数発生手段１２の発生した乱数と特定手段１３の特定した計算式とその変数値とから、ユーザ認証に用いる数値を算出することになる。

【００２４】ここで、ユーザ認証時に応じて変化する変数値としては、ユーザ認証時の年月日（ｙｙｙｙ．ｍｍ．ｄｄ）、時刻（ｈｈ．ｍｍ．ｓｓ）、ＡＭ／ＰＭ（“ＡＭ”＝０、“ＰＭ”＝１など）、曜日（“月曜日”＝１、“火曜日”＝２、・・・など）の一部又は全てを組み合わせて用いることができる。

【００２５】このようにして、本発明のユーザ認証装置１では、ユーザ認証対象に対応した計算式を登録し、乱数を発生してユーザに提示する構成を採って、暗証番号の代わりに、その乱数の提示に応答してユーザから入力される数値と、その計算式とその乱数とから算出される数値との一致をチェックしていくことでユーザ認証を実行する構成を採ることから、ユーザの入力する数値が他人に見られてしまっても秘密性を保持でき、高いセキュリティを実現できるようになる。

【００２６】そして、ネットワーク環境で使用される場合に、ユーザ認証対象に対応した計算式を転送しない構成を採ることで、暗証番号を転送する従来技術に比べて、高いセキュリティを実現できるようになる。

【００２７】しかも、特開昭63-170764 号で開示されたユーザ認証技術に従うと、ユーザは計算式と固有値との両方を覚えなくてはならないのに対して、本発明では、ユーザは計算式のみを覚えれば足りるとともに、特開昭63-170764 号で開示されたユーザ認証技術に従うと、システムは計算式と固有値との両方をメモリに記憶しなければならないのに対して、本発明では、システムは計算式のみを記憶すれば足り、これにより、ユーザやシステムに負荷をかけることなく高いセキュリティを実現できるようになる。

【００２８】そして、本発明のユーザ認証装置１に合わせて、カードの所有者の認証用に用意される本発明のユーザ認証用カードでは、暗証番号に代えて、ユーザ認証対象に対応した計算式を記録する構成を採り、これにより、従来技術よりも高いセキュリティを実現できるようになる。

【００２９】

【発明の実施の形態】以下、実施の形態に従って本発明を詳細に説明する。

【００３０】図２に、本発明を具備する情報処理装置２０の一実施例を図示する。

【００３１】この実施例に従う本発明を具備する情報処理装置２０は、ＣＲＴなどのディスプレイ装置２１と、マウスなどの入力装置２２と、ユーザ認証処理に必要となるデータを格納する認証用管理ファイル２３と、フロッピィディスクや回線などを介してインストールされて、認証用管理ファイル２３の管理データの登録更新処理を実行する認証用管理プログラム２４と、フロッピィディスクや回線などを介してインストールされて、認証用管理ファイル２３の管理データを使ってユーザ認証処理を実行する認証プログラム２５とを備える。

【００３２】図３に、認証用管理ファイル２３の管理データの一実施例を図示する。

【００３３】この図に示すように、認証用管理ファイル２３は、ユーザのＩＤと、そのユーザの登録したパスワードロジック（暗証番号のこともある）との対応関係を管理する。

【００３４】このパスワードロジックは、認証プログラム２５の発生する乱数に対する計算式を定義するものであって、この図の例では、例えば、ユーザＩＤ“０００００５”のユーザは、“ＡＢＣＤ”という数字列で表される乱数に対して、数字Ａと数字Ｂとの差分値を算出するというパスワードロジックを定義して、それを認証用

管理ファイル２３に登録し、また、ユーザＩＤ“０００００４”のユーザは、パスワードロジックの代わりに従前通りの“５３８４”という数字列で表される暗証番号を定義して、それを認証用管理ファイル２３に登録している。

【００３５】図３の実施例では、説明の便宜上、認証用管理ファイル２３に格納されるパスワードロジックを一般的な算術式で記載したが、この計算式は、実際には、例えば逆ポーランド法のような記述形式で記憶されることになる。

【００３６】逆ポーランド法の記述形式に従うと、図中に示す「１０×Ａ」は「１０Ａ＊」、「Ａ×Ａ」は「ＡＡ＊」、「Ａ÷Ｂ」は「ＡＢ／」、「Ａ－Ｂ」は「ＡＢ－」、「（Ｂ－Ａ）＋Ｃ」は「ＢＡ－Ｃ＋」、「((Ａ－Ｂ）×５）÷２」は「ＡＢ－５＊２／」と表される。このような記述形式に従う方のが分かり難いので、セキュリティを高めることができる。

【００３７】図４及び図５に、認証用管理プログラム２４の実行する処理フローの一実施例、図６及び図７に、認証プログラム２５の実行する処理フローの一実施例を図示する。次に、これらの処理フローに従って、図２のように構成される実施例の処理について説明する。

【００３８】認証用管理プログラム２４は、ユーザからパスワードロジックの登録要求が発行されると、図４の処理フローに示すように、先ず最初に、ステップ１で、ディスプレイ装置２１に、図８に示すようなパスワードロジック登録画面を表示する。

【００３９】続いて、ステップ２で、このパスワードロジック登録画面を使ってユーザと対話することで、ユーザＩＤを入力し、続くステップ３で、このパスワードロジック登録画面を使ってユーザと対話することで、ユーザの定義するパスワードロジックを入力する。

【００４０】後述するように、認証プログラム２５は数字列“ＡＢＣＤ”（各数字は０か自然数）で表される４桁の乱数を発生するので、ユーザは、自分のパスワードロジックとして、これらの数字Ａ／数字Ｂ／数字Ｃ／数字Ｄに対する四則演算（全ての数字を使う必要はない。括弧を使うことも許される）を定義することができ、認証用管理プログラム２４は、このユーザの定義するパスワードロジックを入力することになる。ここで、ユーザは、従前通りの暗証番号を使用することを希望するときには、４桁で定義される暗証番号を入力するので、このときには、認証用管理プログラム２４は、このユーザの定義する暗証番号を入力することになる。

【００４１】続いて、ステップ４で、ユーザがパスワードロジック登録画面の終了ボタン（登録実行を指示するボタン）を操作したのか否かを判断して、終了ボタンではなくてキャンセルボタンを操作したことを判断するときには、そのまま処理を終了し、終了ボタンを操作したことを判断するときには、ステップ５に進んで、そのユーザのパスワードロジックが既に認証用管理ファイル２３に登録されているのか否かを判断する。

【００４２】このステップ５の判断処理に従って、そのユーザのパスワードロジックが既に認証用管理ファイル２３に登録されていることを判断するときには、ステップ６に進んで、ステップ３で入力したパスワードロジックの登録不可を表示すべく、ディスプレイ装置２１に、既にパスワードロジックが登録されている旨を出力して処理を終了する。

【００４３】一方、ステップ５で、そのユーザのパスワードロジックが未だ認証用管理ファイル２３に登録されていないことを判断するときには、ステップ７に進んで、ステップ３で入力したパスワードロジックをそのユーザのＩＤと対応をとりつつ、認証用管理ファイル２３に登録して処理を終了する。

【００４４】このようにして、認証用管理プログラム２４は、ユーザからパスワードロジックの登録要求が発行されると、ユーザの定義するパスワードロジックを認証用管理ファイル２３に登録していくように処理するのである。

【００４５】一方、認証用管理プログラム２４は、ユーザから認証用管理ファイル２３に登録したパスワードロジックの更新要求が発行されると、図５の処理フローに示すように、先ず最初に、ステップ１で、ディスプレイ装置２１に、図８に示したようなパスワードロジック登録画面を表示する。

【００４６】続いて、ステップ２で、このパスワードロジック登録画面を使ってユーザと対話することで、ユーザＩＤを入力し、続くステップ３で、このパスワードロジック登録画面を使ってユーザと対話することで、そのユーザが前回登録したパスワードロジックを入力する。

【００４７】続いて、ステップ４で、ユーザがパスワードロジック登録画面のＯＫボタン（前回登録したパスワードロジックの入力完了を示すボタン）を操作するのを待って、ＯＫボタンを操作したことを判断するときには、ステップ５に進んで、認証用管理ファイル２３を参照することで、そのユーザが前回登録したパスワードロジックを取得する。

【００４８】続いて、ステップ６で、ステップ５で取得したパスワードロジックと、ステップ３で入力したパスワードロジックとが一致するのか否かを判断して、一致しないことを判断するときには、前回登録のパスワードロジックを知らなかったことで正規のユーザではないと判断して、パスワードロジックの更新を不許可とすべく、そのまま処理を終了する。

【００４９】一方、ステップ６で、２つのパスワードロジックが一致することを判断するときには、ステップ７に進んで、パスワードロジック登録画面を使ってユーザと対話することで、更新する新たなパスワードロジックを入力する。

【００５０】続いて、ステップ８で、ユーザがパスワードロジック登録画面の終了ボタン（登録実行を指示するボタン）を操作したのか否かを判断して、終了ボタンではなくてキャンセルボタンを操作したことを判断するときには、そのまま処理を終了し、終了ボタンを操作したことを判断するときには、ステップ９に進んで、ステップ７で入力した新たなパスワードロジックに従って、認証用管理ファイル２３に管理されるそのユーザのパスワードロジックを更新して処理を終了する。

【００５１】このようにして、認証用管理プログラム２４は、ユーザからパスワードロジックの更新要求が発行されると、ユーザが認証用管理ファイル２３に管理される前回登録したパスワードロジックを知っていることを条件にして、認証用管理ファイル２３に管理されるパスワードロジックを更新していくように処理するのである。

【００５２】以上に説明した図４及び図５の処理フローに従って、図３に示したように、認証用管理ファイル２３には、ユーザのＩＤと、そのユーザの登録したパスワードロジック（暗証番号のこともある）との対応関係が登録されることになる。

【００５３】この認証用管理ファイル２３の管理データを受けて、ユーザから認証要求要求が発行されると、認証プログラム２５は、図６及び７の処理フローに従って、そのユーザの認証処理を実行する。

【００５４】すなわち、認証プログラム２５は、ユーザから認証要求が発行されると、図６及び図７の処理フローに示すように、先ず最初に、ステップ１で、数字列“ＡＢＣＤ”で表される４桁の乱数を発生し、続くステップ２で、ディスプレイ装置２１に、図９に示すようなパスワード入力画面を表示して、そこに、この発生した乱数をユーザへの提示値として表示する。例えば、“４３６１”という乱数を発生して、これをパスワード入力画面に表示するのである。

【００５５】続いて、ステップ３で、このパスワード入力画面を使ってユーザと対話することで、ユーザＩＤとパスワードとを入力する。

【００５６】このときユーザの入力するパスワードは、認証プログラム２５の発生した４桁の乱数の持つ数字Ａ／数字Ｂ／数字Ｃ／数字Ｄを、そのユーザが認証用管理ファイル２３に登録したパスワードロジックに代入することで求められることになる。例えば、認証プログラム２５が“４３６１”という乱数を発生するときに、ユーザが「Ａ＋Ｂ＋Ｃ＋Ｄ」というパスワードロジックを登録しているときには、ユーザは、「４＋３＋６＋１」により求められる“１４”というパスワードを求めて、それをパスワード入力画面に入力することになる。

【００５７】このとき、認証プログラム２５は、パスワードロジックに分母が“０”となる割算が存在するときには、その割算結果を“０”として扱うという規約にしているので、ユーザは、その規約に従ってパスワードを算出することになる。また、認証プログラム２５は、パスワードロジックに剰余のでる割算が存在するときには、小数点以下を切り捨てるという規約にしているので、ユーザは、その規約に従ってパスワードを算出することになる。また、認証プログラム２５は、パスワードロジックの演算結果が負となるときには、その演算結果の絶対値をとるという規約にしているので、ユーザは、その規約に従ってパスワードを算出することになる。

【００５８】また、ユーザは、認証用管理ファイル２３に従前通りの暗証番号を登録しているときには、その暗証番号をそのままパスワードとして、パスワード入力画面に入力することになる。

【００５９】このようにして、ステップ３で、ユーザからユーザＩＤ及びパスワードを入力すると、続いて、ステップ４で、その入力したユーザＩＤが認証用管理ファイル２３に登録されているのか否かを判断して、登録されていることを判断するときには、ステップ５に進んで、認証用管理ファイル２３を参照することで、そのユーザの登録したパスワードロジックを取得する。

【００６０】続いて、ステップ６で、ステップ１で発生した乱数を分解することで、数字Ａ／数字Ｂ／数字Ｃ／数字Ｄの値を得る。続いて、ステップ７で、その得た値をステップ５で取得したパスワードロジックに代入することで、ユーザの入力したパスワードに対応する演算値を算出する。

【００６１】このとき、認証プログラム２５は、パスワードロジックに分母が“０”となる割算が存在するときには、その割算結果を“０”として扱うという規約に従って演算値を算出し、パスワードロジックに剰余のでる割算が存在するときには、小数点以下を切り捨てるという規約に従って演算値を算出し、パスワードロジックの演算結果が負となるときには、その演算結果の絶対値をとるという規約に従って演算値を算出し、パスワードロジックとして従前通りの暗証番号が登録されているときには、その暗証番号をそのまま演算値として算出していくように処理する。

【００６２】続いて、ステップ８で、ステップ３で入力したパスワードと、ステップ７で算出した演算値とを照合することでユーザ認証処理を実行し、続くステップ９で、その照合により２つのパスワードの一致が検出されたのか否かを判断して、２つのパスワードの一致が検出されるときには、ステップ１０に進んで、図示しない業務プログラムに対してユーザ認証完了を出力することで、その業務プログラムに対して処理に入ることを指示する。

【００６３】一方、ステップ４で、入力したユーザＩＤが認証用管理ファイル２３に登録されていないことを判断するときと、ステップ９で、２つのパスワードが一致しないことが検出されるときには、ステップ１１（図９

の処理フロー）に進んで、ユーザ認証処理を規定回数トライしたのか否かを判断して、規定回数トライしたことを判断するときには、ステップ１２に進んで、ディスプレイ装置２１に、ユーザ認証エラーを出力して処理を終了する。

【００６４】そして、ステップ１１で、ユーザ認証処理を規定回数トライしていないことを判断するときには、ステップ１３に進んで、トライ回数を１つカウントアップしてから、ステップ１に戻っていくことで、上述のユーザ認証処理を再度実行していく。

【００６５】このようにして、認証プログラム２５は、ユーザから認証要求が発行されると、図６及び図７の処理フローに従って、認証用管理ファイル２３に登録されたユーザ定義のパスワードロジックとユーザに提示する乱数とから算出される演算値と、その乱数の提示に応答してユーザが入力してくるパスワードとが一致するのか否かをチェックしていくことで、ユーザ認証処理を実行するように処理するのである。

【００６６】このユーザ認証処理に従って、ユーザの入力する数値が他人に見られてしまっても秘密性を保持でき、高いセキュリティを実現できるようになる。そして、ユーザはパスワードロジックのみを覚えれば足りるとともに、システムはパスワードロジックのみを記憶すれば足り、これにより、ユーザやシステムに負荷をかけることなく高いセキュリティを実現できるようになる。

【００６７】しかも、従来技術で用いる暗証番号によるユーザ認証処理もそのまま併用できることから、暗証番号を用いたいと希望するユーザの要望にもそのまま対応できることになる。

【００６８】図１０に、本発明の他の実施例を図示する。

【００６９】この実施例は、ネットワーク環境で動作する流通管理システムに対して、本発明を適用したものである。

【００７０】この実施例に従う本発明を具備する流通管理システムは、ユーザ認証処理を実行する認証用サーバ３０と、流通側に設置される複数の流通端末４０と、認証用サーバ３０と流通端末４０との間を接続するネットワーク５０とで構成されている。

【００７１】この認証用サーバ３０は、図２に示した認証用管理ファイル２３と同一のデータを管理する認証用管理ファイル３１と、フロッピィディスクや回線などを介してインストールされて、認証用管理ファイル３１の管理データの登録更新処理を実行する認証用管理プログラム３２と、フロッピィディスクや回線などを介してインストールされて、認証用管理ファイル３１の管理データを使ってユーザ認証処理を実行する認証プログラム３３とを備える。

【００７２】一方、流通端末４０は、ＣＲＴなどのディスプレイ装置４１と、マウスなどの入力装置４２と、フロッピィディスクや回線などを介してインストールされて、ユーザ認証処理のための対話処理を実行する対話プログラム４３とを備える。

【００７３】図１１／図１３／図１４／図１７に、対話プログラム４３の実行する処理フローの一実施例、図１２／図１５／図１６に、認証用管理プログラム３２の実行する処理フローの一実施例、図１８に、認証プログラム３３の実行する処理フローの一実施例を図示する。次に、これらの処理フローに従って、図１０のように構成される実施例の処理について説明する。

【００７４】先ず最初に、図１１及び図１２の処理フローに従って、認証用管理ファイル３１に対するパスワードロジックの登録処理について説明する。

【００７５】流通端末４０に展開される対話プログラム４３は、ユーザから認証用管理ファイル３１に対するパスワードロジックの登録要求が発行されると、図１１の処理フローに示すように、先ず最初に、ステップ１で、ディスプレイ装置４１に、図８に示したようなパスワードロジック登録画面を表示する。

【００７６】続いて、ステップ２で、このパスワードロジック登録画面を使ってユーザと対話することで、ユーザＩＤを入力し、続くステップ３で、このパスワードロジック登録画面を使ってユーザと対話することで、ユーザの定義するパスワードロジック（図２の実施例で入力したパスワードロジックと同じもの）を入力する。

【００７７】続いて、ステップ４で、ユーザがパスワードロジック登録画面の終了ボタン（登録実行を指示するボタン）を操作したのか否かを判断して、終了ボタンではなくてキャンセルボタンを操作したことを判断するときには、そのまま処理を終了し、終了ボタンを操作したことを判断するときには、ステップ５に進んで、入力したユーザＩＤとパスワードロジックとを認証用管理プログラム３２に送信する。

【００７８】後述するように、認証用管理プログラム３２は、この送信に応答して、対話プログラム４３の送信したパスワードロジックの登録ができたのか否かを示す情報を返信してくるので、続いて、ステップ６で、認証用管理プログラム３２からの返信情報を待って、この返信情報を受け取ると、続くステップ７で、この返信情報がパスワードロジックの登録完了を示す情報であるのか否かを判断する。

【００７９】この判断処理に従って、認証用管理プログラム３２からパスワードロジックの登録完了を示す情報が返信されてきたことを判断するときには、そのまま処理を終了し、登録できない旨の情報が返信されてきたことを判断するときには、ステップ８に進んで、ディスプレイ装置４１に、パスワードロジックを登録できない旨を出力して処理を終了する。

【００８０】この図１１の処理フローで示した対話プログラム４３の処理を受けて、認証用サーバ３０に展開さ

れる認証用管理プログラム３２は、対話プログラム４３がパスワードロジックの登録要求を発行すると、図１２の処理フローに示すように、先ず最初に、ステップ１で、対話プログラム４３から送られてくるユーザＩＤと登録要求のパスワードロジックとを受け取る。

【００８１】続いて、ステップ２で、その受け取ったユーザＩＤの指すユーザのパスワードロジックが既に認証用管理ファイル３１に登録されているのか否かを判断して、既に登録されていることを判断するときには、ステップ３に進んで、対話プログラム４３に対して、登録要求のパスワードロジックを登録できない旨を返信して処理を終了する。

【００８２】一方、ステップ２で、受け取ったユーザＩＤの指すユーザのパスワードロジックが認証用管理ファイル３１に登録されていないことを判断するときには、ステップ４に進んで、受け取った登録要求のパスワードロジックを受け取ったユーザＩＤと対応をとりつつ、認証用管理ファイル３１に登録し、続くステップ５で、対話プログラム４３に対して、登録要求のパスワードロジックの登録を完了した旨を返信して処理を終了する。

【００８３】このようにして、対話プログラム４３と認証用管理プログラム３２とは、ユーザからパスワードロジックの登録要求が発行されると、ネットワーク５０を介して連携処理を実行しつつ、ユーザの定義するパスワードロジックを認証用管理ファイル３１に登録していくように処理するのである。

【００８４】次に、図１３ないし図１６の処理フローに従って、認証用管理ファイル３１に管理されるパスワードロジックの更新処理について説明する。

【００８５】流通端末４０に展開される対話プログラム４３は、ユーザから認証用管理ファイル３１に登録したパスワードロジックの更新要求が発行されると、図１３の処理フローに示すように、先ず最初に、ステップ１で、ディスプレイ装置４１に、図８に示したようなパスワードロジック登録画面を表示する。

【００８６】続いて、ステップ２で、このパスワードロジック登録画面を使ってユーザと対話することで、ユーザＩＤを入力し、続くステップ３で、このパスワードロジック登録画面を使ってユーザと対話することで、そのユーザが前回登録したパスワードロジックを入力する。

【００８７】続いて、ステップ４で、ユーザがパスワードロジック登録画面のＯＫボタン（前回登録したパスワードロジックの入力完了を示すボタン）を操作するのを待って、ＯＫボタンを操作したことを判断するときには、ステップ５に進んで、入力したユーザＩＤとパスワードロジック（ユーザが前回登録したもの）とを認証用管理プログラム３２に送信する。

【００８８】後述するように、認証用管理プログラム３２は、この送信に応答して、対話プログラム４３の発行するパスワードロジックの更新要求が実行できるのか否かを示す情報を返信してくるので、続いて、ステップ６で、認証用管理プログラム３２からの返信情報を待って、この返信情報を受け取ると、続くステップ７で、この返信情報がパスワードロジックの更新の可能を示す情報であるのか否かを判断する。

【００８９】この判断処理に従って、認証用管理プログラム３２からパスワードロジックの更新不可能を示す情報が返信されてきたことを判断するときには、ステップ８に進んで、ディスプレイ装置４１に、パスワードロジックを更新できない旨を出力して処理を終了する。

【００９０】一方、ステップ７で、認証用管理プログラム３２からパスワードロジックの更新可能を示す情報が返信されてきたことを判断するときには、ステップ９に進んで、パスワードロジック登録画面を使ってユーザと対話することで、更新する新たなパスワードロジックを入力する。

【００９１】続いて、ステップ１０（図１４の処理フロー）で、ユーザがパスワードロジック登録画面の終了ボタン（登録実行を指示するボタン）を操作したのか否かを判断して、終了ボタンではなくてキャンセルボタンを操作したことを判断するときには、そのまま処理を終了し、終了ボタンを操作したことを判断するときには、ステップ１１に進んで、ユーザＩＤとステップ９で入力したパスワードロジック（更新要求のもの）とを認証用管理プログラム３２に送信する。

【００９２】後述するように、認証用管理プログラム３２は、この送信に応答して、対話プログラム４３の送信したパスワードロジックの登録ができたことを示す情報を返信してくるので、続いて、ステップ１２で、認証用管理プログラム３２からの返信情報を待って、この返信情報を受け取ると、処理を終了する。

【００９３】この図１３及び図１４の処理フローに示した対話プログラム４３の処理を受けて、認証用サーバ３０に展開される認証用管理プログラム３２は、対話プログラム４３がパスワードロジックの更新要求を発行すると、図１５及び図１６の処理フローに示すように、先ず最初に、ステップ１で、対話プログラム４３から送られてくるユーザＩＤと前回登録のパスワードロジックとを受け取る。

【００９４】続いて、ステップ２で、認証用管理ファイル３１を参照することで、その受け取ったユーザＩＤの指すパスワードロジックを取得する。続いて、ステップ３で、ステップ２で取得したパスワードロジックと、ステップ１で受け取ったパスワードロジックとが一致するのか否かを判断して、一致しないことを判断するときには、ステップ４に進んで、対話プログラム４３に対して、パスワードロジックを更新できない旨を返信して処理を終了する。

【００９５】一方、ステップ３で、２つのパスワードロジックが一致することを判断するときには、ステップ５

に進んで、対話プログラム４３に対して、パスワードロジックを更新できる旨を返信する。

【００９６】上述したように、対話プログラム４３は、認証用管理プログラム３２からパスワードロジックの更新が可能である旨の通知を受け取ると、ユーザＩＤと更新要求のパスワードロジックとを送信してくるので、続いて、ステップ６で、対話プログラム４３から、ユーザＩＤと更新要求のパスワードロジックとが送られてくるのを待って、それを受け取る。

【００９７】続いて、ステップ７（図１６の処理フロー）で、その受け取った更新要求のパスワードロジックに従って、認証用管理ファイル３１に管理されるその受け取ったユーザＩＤの指すパスワードロジックを更新し、続くステップ８で、対話プログラム４３に対して、パスワードロジックの更新完了を通知して処理を終了する。

【００９８】このようにして、対話プログラム４３と認証用管理プログラム３２とは、ユーザからパスワードロジックの更新要求が発行されると、ネットワーク５０を介して連携処理を実行しつつ、ユーザが前回登録のパスワードロジックを知っていることを条件にして、認証用管理ファイル３１に管理されるパスワードロジックを更新していくように処理するのである。

【００９９】以上に説明した図１１ないし図１６の処理フローに従って、図３に示したように、認識用サーバ３０の備える認証用管理ファイル３１には、ユーザのＩＤと、そのユーザの登録したパスワードロジック（暗証番号のこともある）との対応関係が登録されることになる。

【０１００】この認証用管理ファイル３１の管理データを受けて、ユーザから認証要求が発行されると、対話プログラム４３と認証用管理プログラム３２とは、ネットワーク５０を介して連携処理を実行しつつ、そのユーザの認証処理を実行する。

【０１０１】次に、図１７及び図１８の処理フローに従って、このとき実行されるユーザ認証処理について説明する。

【０１０２】流通端末４０に展開される対話プログラム４３は、ユーザからユーザ認証処理の実行要求が発行されると、図１７の処理フローに示すように、先ず最初に、ステップ１で、数字列“ＡＢＣＤ”で表される４桁の乱数を発生し、続くステップ２で、ディスプレイ装置４１に、図９に示したようなパスワード入力画面を表示して、そこに、この発生した乱数をユーザへの提示値として表示する。例えば、“４３６１”という乱数を発生して、これをパスワード入力画面に表示するのである。

【０１０３】なお、後述することからも分かるように、このとき発生する乱数は４桁である必要はなく、１桁や２桁や３桁であってもよく、更に大きな桁数であってもよい。

【０１０４】続いて、ステップ３で、このパスワード入力画面を使ってユーザと対話することで、ユーザＩＤとパスワードとを入力する。

【０１０５】このときユーザの入力するパスワードは、対話プログラム４３の発生した４桁の乱数の持つ数字Ａ／数字Ｂ／数字Ｃ／数字Ｄを、そのユーザが認証用管理ファイル４１に登録したパスワードロジックに代入することで求められることになる。このとき、ユーザは、パスワードロジックに分母が“０”となる割算が存在するときには、その割算結果を“０”として算出するという規約に従ってパスワードを算出し、パスワードロジックに剰余のでる割算が存在するときには、小数点以下を切り捨てるという規約に従ってパスワードを算出し、パスワードロジックの演算結果が負となるときには、その演算結果の絶対値をとるという規約に従ってパスワードを算出することになる。また、ユーザは、認証用管理ファイル４１に従前通りの暗証番号を登録しているときには、その暗証番号をそのままパスワードとして、パスワード入力画面に入力することになる。

【０１０６】このようにして、ステップ３で、ユーザＩＤ及びパスワードを入力すると、続いて、ステップ４で、ステップ１で発生した乱数と、ステップ３で入力したユーザＩＤ／パスワードとを認証プログラム３３に送信する。

【０１０７】後述するように、認証プログラム３３は、この送信に応答して、対話プログラム４３の発行するパスワードに従ってユーザを認証できたのか否かを示す情報を返信してくるので、続いて、ステップ５で、認証プログラム３３からの返信情報を待って、この返信情報を受け取ると、続くステップ６で、この返信情報がユーザ認証の完了を示す情報であるのか否かを判断する。

【０１０８】この判断処理に従って、認証プログラム３３からユーザ認証の完了を示す情報が返信されてきたことを判断するときには、ステップ７に進んで、図示しない業務プログラムに対してユーザ認証完了を出力することで、その業務プログラムに対して処理に入ることを指示する。

【０１０９】一方、ステップ６で、認証プログラム３３からユーザ認証の不可能を示す情報が返信されてきたことを判断するときには、ステップ８に進んで、ユーザ認証処理を規定回数トライしたのか否かを判断して、ユーザ認証処理を規定回数トライしたことを判断するときには、ステップ９に進んで、ディスプレイ装置４１に、ユーザ認証エラーを出力して処理を終了する。

【０１１０】そして、ステップ８で、ユーザ認証処理を規定回数トライしていないことを判断するときには、ステップ１０に進んで、トライ回数を１つカウントアップしてから、ステップ１に戻っていくことで、上述のユーザ認証処理を再度実行していく。

【０１１１】この図１７の処理フローに示した対話プロ

グラム４３の処理を受けて、認証用サーバ３０に展開される認証プログラム３３は、対話プログラム４３がユーザ認証処理の実行要求を発行すると、図１８の処理フローに示すように、先ず最初に、ステップ１で、対話プログラム４３から送られてくる、乱数とユーザＩＤとパスワードロジックとを受け取る。

【０１１２】続いて、ステップ２で、その受け取ったユーザＩＤが認証用管理ファイル３１に登録されているのか否かを判断して、登録されていることを判断するときには、ステップ３に進んで、認証用管理ファイル３１を参照することで、そのユーザＩＤの指すパスワードロジックを取得する。

【０１１３】続いて、ステップ４で、ステップ１で受け取った乱数を分解することで、数字Ａ／数字Ｂ／数字Ｃ／数字Ｄの値を得る。続いて、ステップ５で、その得た値をステップ３で取得したパスワードロジックに代入することで、ユーザの入力したパスワードに対応する演算値を算出する。

【０１１４】このとき、認証プログラム３３は、パスワードロジックに分母が“０”となる割算が存在するときには、その割算結果を“０”として扱うという規約に従って演算値を算出し、パスワードロジックに剰余のでる割算が存在するときには、小数点以下を切り捨てるという規約に従って演算値を算出し、パスワードロジックの演算結果が負となるときには、その演算結果の絶対値をとるという規約に従って演算値を算出し、パスワードロジックとして従前通りの暗証番号が登録されているときには、その暗証番号をそのまま演算値として算出していくように処理する。

【０１１５】続いて、ステップ６で、ステップ１で受け取ったパスワードと、ステップ５で算出した演算値とを照合することでユーザ認証処理を実行し、続くステップ７で、その照合により２つのパスワードの一致が検出されたのか否かを判断して、２つのパスワードの一致が検出されるときには、ステップ８に進んで、対話プログラム４３に対してユーザ認証完了を返信して、処理を終了する。

【０１１６】一方、ステップ２で、対話プログラム４３から受け取ったユーザＩＤが認証用管理ファイル３１に登録されていないことを判断するときと、ステップ７で、２つのパスワードが一致しないことが検出されるときには、ステップ９に進んで、対話プログラム４３に対してユーザ認証エラーを返信して、処理を終了する。

【０１１７】このようにして、対話プログラム４３と認証プログラム３３とは、ユーザから認証要求要求が発行されると、図１７及び図１８の処理フローに従って、ネットワーク５０を介して連携処理を実行しつつ、認証用管理ファイル３２に登録されたユーザ定義のパスワードロジックとユーザに提示する乱数とから算出される演算値と、その乱数の提示に応答してユーザが入力してくるパスワードとが一致するのか否かをチェックしていくことで、ユーザ認証処理を実行するように処理するのである。

【０１１８】このユーザ認証処理に従って、ユーザの入力する数値が他人に見られてしまっても秘密性を保持でき、高いセキュリティを実現できるようになる。そして、ユーザはパスワードロジックのみを覚えれば足りるとともに、システムはパスワードロジックのみを記憶すれば足り、これにより、ユーザやシステムに負荷をかけることなく高いセキュリティを実現できるようになる。

【０１１９】更に、暗証番号に相当するパスワードロジックについては、それが認証用管理ファイル３２に登録される場合を除きネットワーク５０に転送されることがないことで盗み見られるという危険性がなく、これにより高いセキュリティを実現できるようになる。

【０１２０】ここで、図１７及び図１８の処理フローでは、対話プログラム４３が乱数を発生していく構成を採ったが、認証プログラム３３が乱数を発生して、それを対話プログラム４３に通知していくという構成を採ることも可能である。

【０１２１】以上に説明したように、本発明は、ユーザ定義のパスワードロジックを登録し、乱数を発生してユーザに提示する構成を採って、暗証番号の代わりに、その乱数の提示に応答してユーザから入力される数値と、そのパスワードロジックとその乱数とから算出される数値との一致をチェックしていくことでユーザ認証を実行する構成を採ることを、基本的な技術思想としている。

【０１２２】この技術思想に従って、本発明では、磁気カードやＩＣカードなどのようなユーザ認証用カードに、暗証番号に代えて、上述したようなユーザ定義のパスワードロジックを記録していく構成を採ることになる。

【０１２３】すなわち、従来の磁気カードやＩＣカードなどのユーザ認証用カードでは、ユーザＩＤと暗証番号とを記録する構成を採るのに対して、本発明を具備するユーザ認証用カードでは、ユーザＩＤとユーザ定義のパスワードロジックとを記録する構成を採ることになる。

【０１２４】図１９に、本発明を具備するＩＣカード６０の一実施例を図示する。

【０１２５】この図に示すように、本発明を具備するＩＣカード６０は、メモリ部６００に、ユーザＩＤとユーザ定義のパスワードロジックとを記録するとともに、乱数発生機構６０１を備える構成を採る。

【０１２６】このように構成される本発明を具備するＩＣカード６０は、流通端末４０の備えるＩＣカードリーダ７０にセットされ、一方、流通端末４０には、このＩＣカード６０に記録されるパスワードロジックを使って、ユーザ認証処理を実行するカード認証プログラム４４が備えられることになる。

【０１２７】図２０及び図２１に、このカード認証プロ

グラム４４の実行する処理フローの一実施例を図示する。次に、この処理フローに従って、本発明を具備するＩＣカード６０に適用されるユーザ認証処理について説明する。

【０１２８】流通端末４０に展開されるカード認証プログラム４４は、本発明を具備するＩＣカード６０に対するユーザ認証要求が発行されると、図２０及び図２１の処理フローに示すように、先ず最初に、ステップ１で、ＩＣカード６０に記録されるユーザＩＤとパスワードロジックとを読み取る。

【０１２９】続いて、ステップ２で、ＩＣカード６０の乱数発生機構６０１が発生する４桁の乱数を入力する。続いて、ステップ３で、図９に示すようなパスワード入力画面を表示して、そこに、この入力した乱数をユーザへの提示値として表示する。例えば、“４３６１”という乱数を発生して、これをパスワード入力画面に表示するのである。

【０１３０】続いて、ステップ４で、このパスワード入力画面を使ってユーザと対話することで、パスワードを入力する。

【０１３１】このときユーザの入力するパスワードは、乱数発生機構６０１の発生した４桁の乱数の持つ数字Ａ／数字Ｂ／数字Ｃ／数字Ｄを、ＩＣカード６０に記録されるパスワードロジックに代入することで求められることになる。このとき、ユーザは、パスワードロジックに分母が“０”となる割算が存在するときには、その割算結果を“０”として算出するという規約に従ってパスワードを算出し、パスワードロジックに剰余のでる割算が存在するときには、小数点以下を切り捨てるという規約に従ってパスワードを算出し、パスワードロジックの演算結果が負となるときには、その演算結果の絶対値をとるという規約に従ってパスワードを算出することになる。また、ユーザは、ＩＣカード６０が従前通りの暗証番号を記録しているときには、その暗証番号をそのままパスワードとして、パスワード入力画面に入力することになる。

【０１３２】このようにして、ステップ４で、ユーザからパスワードを入力すると、続いて、ステップ５で、ステップ１で読み取った乱数を分解することで、数字Ａ／数字Ｂ／数字Ｃ／数字Ｄの値を得る。続いて、ステップ６で、その得た値をステップ１で読み取ったパスワードロジックに代入することで、ユーザの入力したパスワードに対応する演算値を算出する。

【０１３３】続いて、ステップ７で、ステップ４で入力したパスワードと、ステップ６で算出した演算値とを照合することでユーザ認証処理を実行し、続くステップ８で、その照合により２つのパスワードの一致が検出されたのか否かを判断して、２つのパスワードの一致が検出されるときには、ステップ９に進んで、図示しない業務プログラムに対してユーザ認証完了を出力することで、その業務プログラムに対して処理に入ることを指示する。

【０１３４】一方、ステップ８で、２つのパスワードが一致しないことが検出されるときには、ステップ１０に進んで、ユーザ認証処理を規定回数トライしたのか否かを判断して、ユーザ認証処理を規定回数トライしたことを判断するときには、ステップ１１（図２１の処理フロー）に進んで、ディスプレイ装置４１に、ユーザ認証エラーを出力して処理を終了する。

【０１３５】そして、ステップ１０で、ユーザ認証処理を規定回数トライしていないことを判断するときには、ステップ１２（図２１の処理フロー）に進んで、トライ回数を１つカウントアップしてから、ステップ１に戻っていくことで、上述のユーザ認証処理を再度実行していく。

【０１３６】このようにして、本発明では、磁気カードやＩＣカードなどのようなユーザ認証用カードに、暗証番号に代えて、上述したようなユーザ定義のパスワードロジックを記録する構成を採る。そして、ユーザ認証用カードに記録されたユーザ定義のパスワードロジックとユーザに提示する乱数とから算出される演算値と、その乱数の提示に応答してユーザが入力してくるパスワードとが一致するのか否かをチェックしていくことで、ユーザ認証処理を実行するように処理するのである。

【０１３７】このユーザ認証処理に従って、ユーザの入力する数値が他人に見られてしまっても秘密性を保持でき、高いセキュリティを実現できるようになる。

【０１３８】なお、図１９に示した実施例では、ＩＣカード６０に乱数発生機構６０１を備える構成を採ったが、この乱数発生機能については、カード認証プログラム４４の方に備えるという構成を採ることも可能である。

【０１３９】以上に説明した実施例では、乱数の持つ数字に対する四則演算で定義されるパスワードロジックを開示したが、この乱数の持つ数字の他に、カレンダー情報や時刻情報などのような全ユーザ及びシステムが一義的に決定できる変数値を含めることも可能である。

【０１４０】例えば、１月～１２月に対して、“１”～“１２”という変数値ｎを割り付けたり、０時～２４時に対して、“０”～“２４”という変数値ｎを割り付けたりして、例えば、「（Ａ－Ｂ）＋ｎ」というように、乱数の持つ数字の他に、この変数値ｎを含める形でパスワードロジックを定義することも可能である。

【０１４１】

【発明の効果】以上説明したように、本発明では、ユーザ定義の計算式を登録し、乱数を発生してユーザに提示する構成を採って、暗証番号の代わりに、その乱数の提示に応答してユーザから入力される数値と、その計算式とその乱数とから算出される数値との一致をチェックしていくことでユーザ認証を実行する構成を採ることか

ら、ユーザの入力する数値が他人に見られてしまっても秘密性を保持でき、高いセキュリティを実現できるようになる。

【０１４２】そして、ネットワーク環境で使用される場合に、ユーザ定義の計算式を転送しない構成を採ることで、暗証番号を転送する従来技術に比べて、高いセキュリティを実現できるようになる。

【０１４３】しかも、特開昭63-170764 号で開示されたユーザ認証技術に従うと、ユーザは計算式と固有値との両方を覚えなくてはならないのに対して、本発明では、ユーザは計算式のみを覚えれば足りるとともに、特開昭63-170764 号で開示されたユーザ認証技術に従うと、システムは計算式と固有値との両方をメモリに記憶しなければならないのに対して、本発明では、システムは計算式のみを記憶すれば足り、これにより、ユーザやシステムに負荷をかけることなく高いセキュリティを実現できるようになる。

【０１４４】そして、本発明では、カードの所有者の認証用に用意されるカードに、暗証番号に代えて、ユーザ定義の計算式を記録する構成を採ることで、従来技術よりも高いセキュリティを実現できるようになる。

【図面の簡単な説明】

【図１】本発明の原理構成図である。

【図２】本発明の一実施例である。

【図３】認証用管理ファイルの一実施例である。

【図４】認証用管理プログラムの処理フローである。

【図５】認証用管理プログラムの処理フローである。

【図６】認証プログラムの処理フローである。

【図７】認証プログラムの処理フローである。

【図８】パスワードロジック登録画面の一実施例である。

【図９】パスワード入力画面の一実施例である。

【図１０】本発明の他の実施例である。

【図１１】対話プログラムの処理フローである。

【図１２】認証用管理プログラムの処理フローである。

【図１３】対話プログラムの処理フローである。

【図１４】対話プログラムの処理フローである。

【図１５】認証用管理プログラムの処理フローである。

【図１６】認証用管理プログラムの処理フローである。

【図１７】対話プログラムの処理フローである。

【図１８】認証プログラムの処理フローである。

【図１９】本発明の一実施例である。

【図２０】カード認証プログラムの処理フローである。

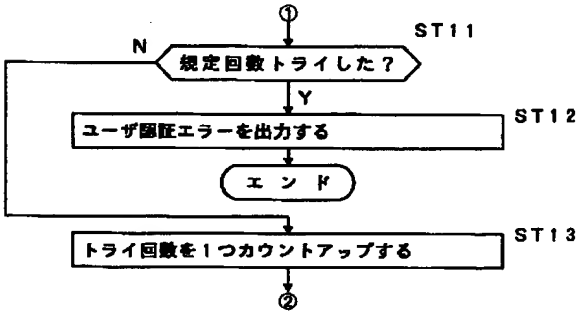
【図２１】カード認証プログラムの処理フローである。

【符号の説明】

1　ユーザ認証装置
2　端末
１０　管理手段
１１　登録更新手段
１２　乱数発生手段
１３　特定手段
１４　算出手段
１５　判断手段

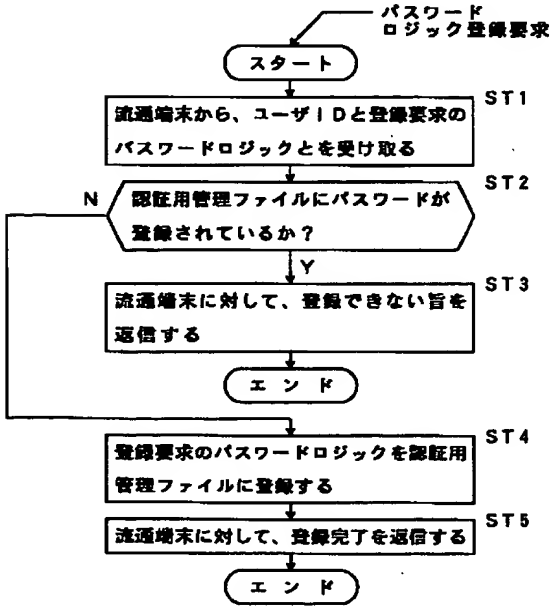
【図７】

認証プログラムの処理フロー



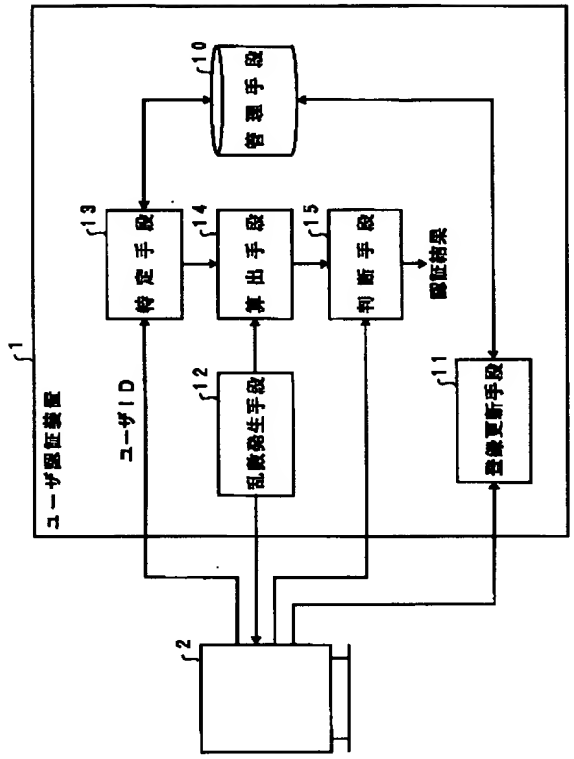
【図１２】

認証用管理プログラムの処理フロー



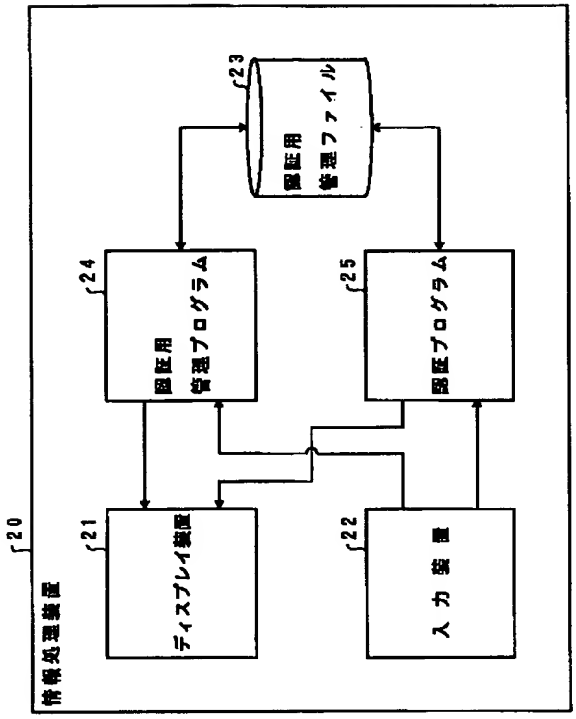
【図１】

本発明の原理構成図



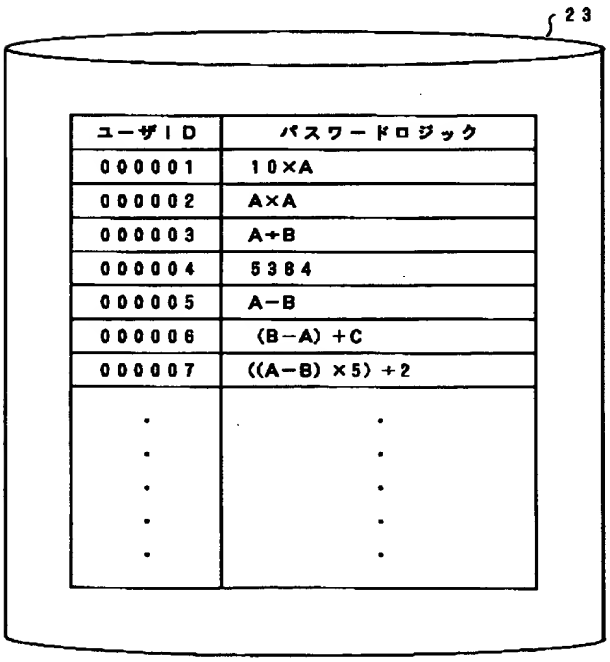
【図２】

本発明の一実施例



【図３】

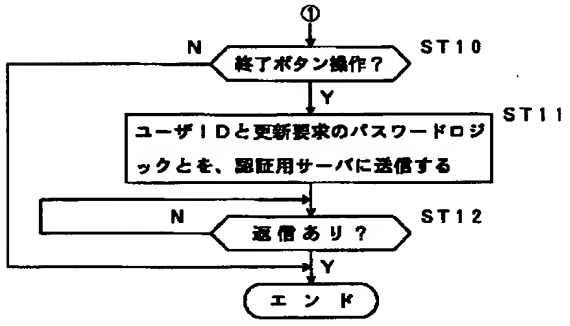
認証用管理ファイルの一実施例



ユーザＩＤ	パスワードロジック
000001	10×A
000002	A×A
000003	A+B
000004	5384
000005	A−B
000006	(B−A)＋C
000007	((A−B)×5)＋2
・	・
・	・
・	・
・	・
・	・

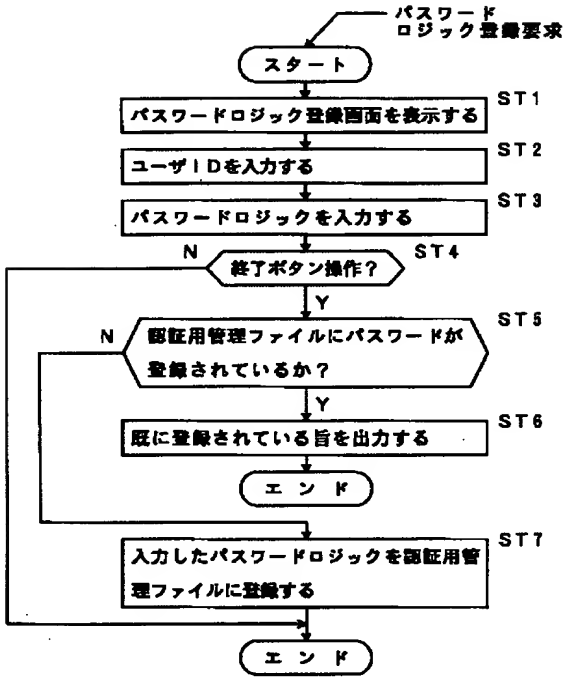
【図１４】

対話プログラムの処理フロー



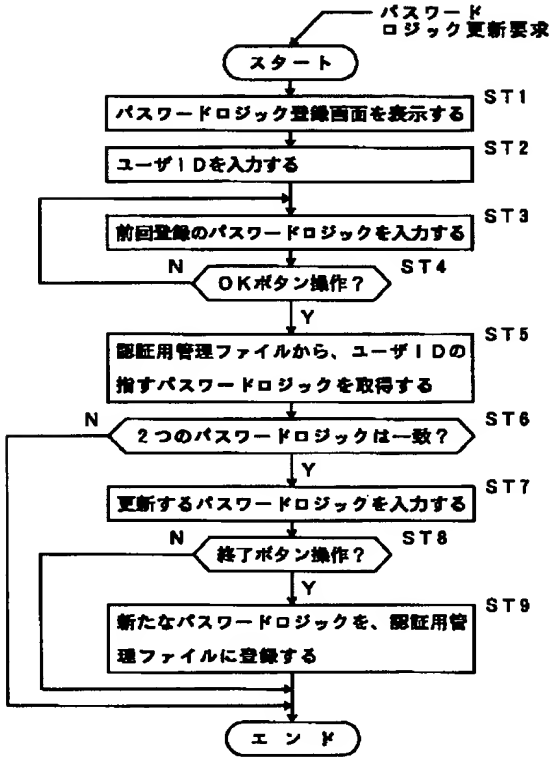
【図４】

認証用管理プログラムの処理フロー



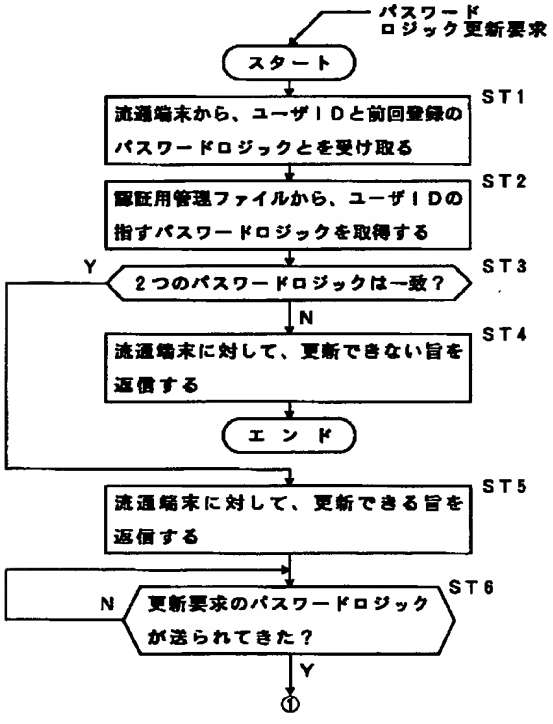
【図５】

認証用管理プログラムの処理フロー



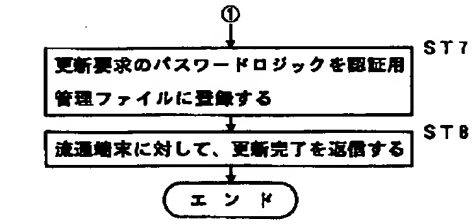
【図１５】

認証用管理プログラムの処理フロー



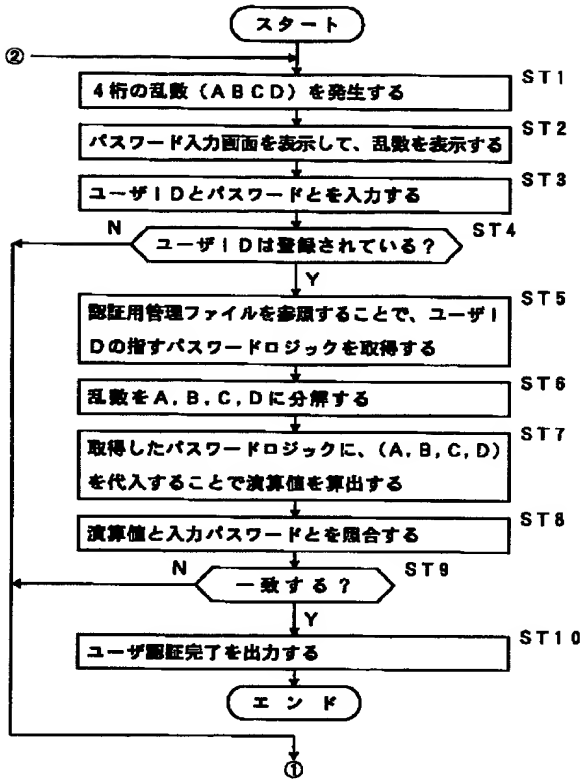
【図１６】

認証用管理プログラムの処理フロー



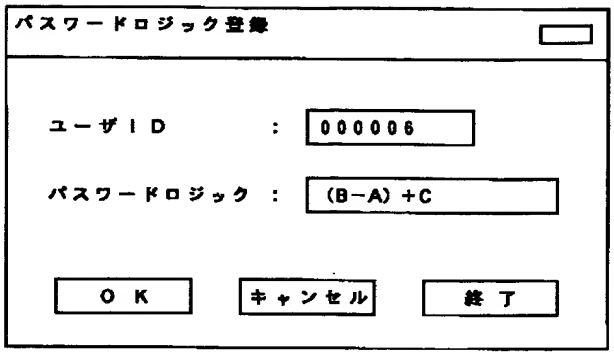
【図６】

認証プログラムの処理フロー



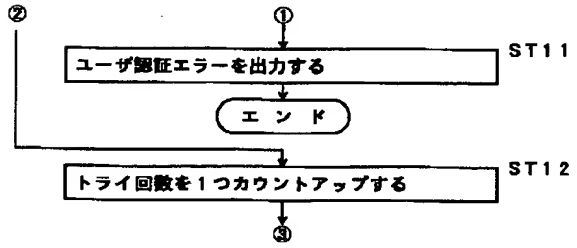
【図８】

パスワードロジック登録画面の一実施例



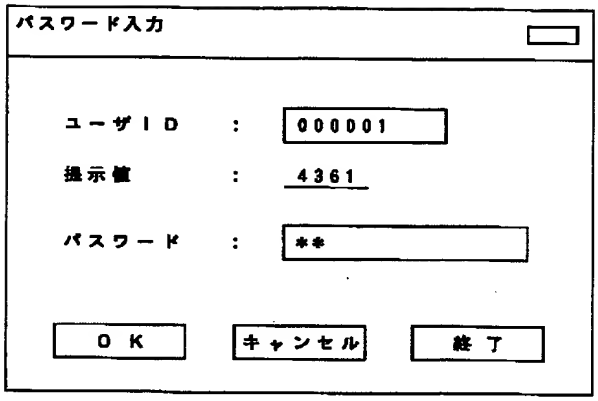
【図２１】

カード認証プログラムの処理フロー



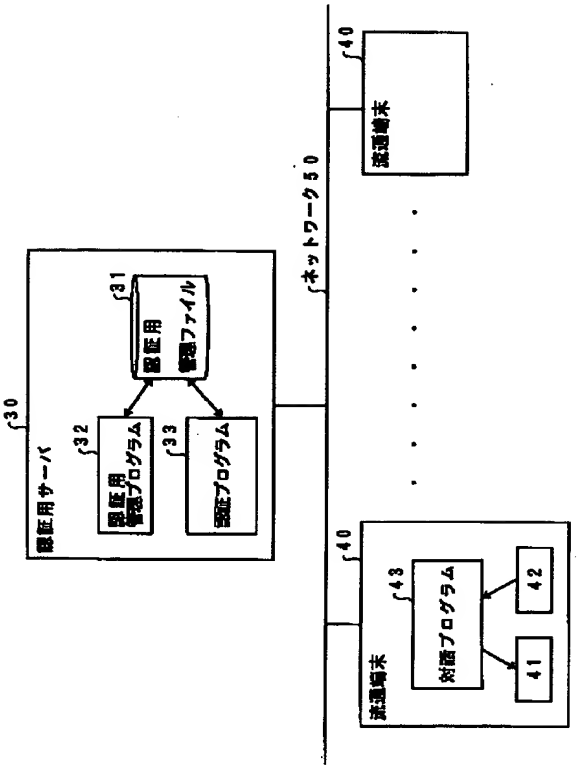
【図９】

パスワード入力画面の一実施例



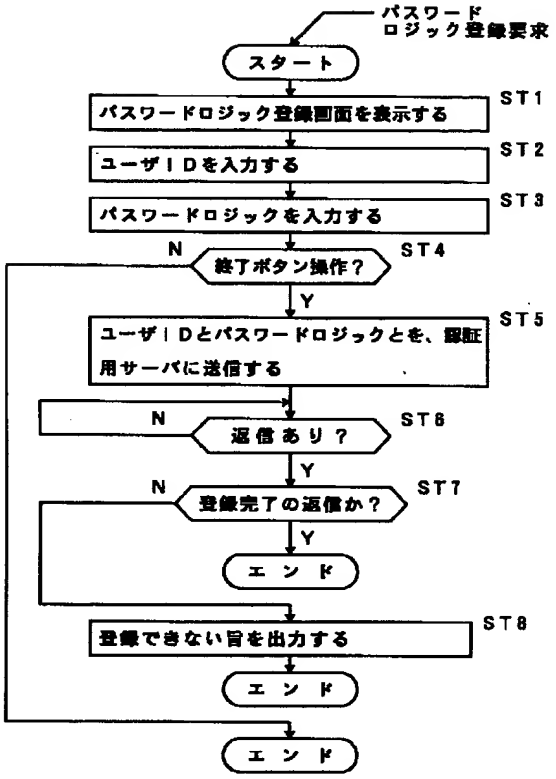
【図１０】

本発明の他の実施例



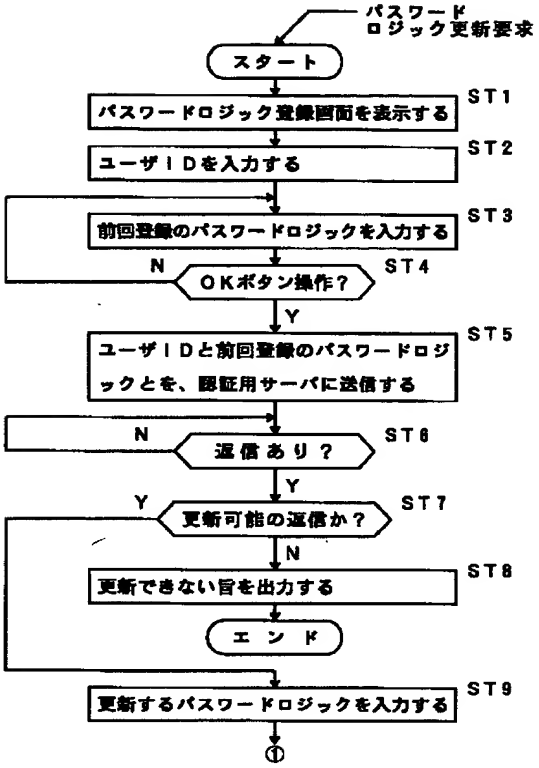
【図１１】

対話プログラムの処理フロー



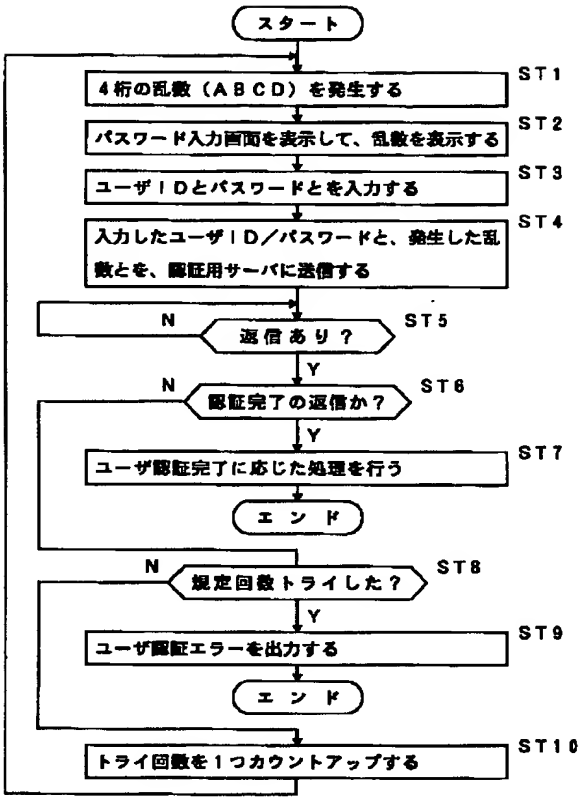
【図１３】

対話プログラムの処理フロー



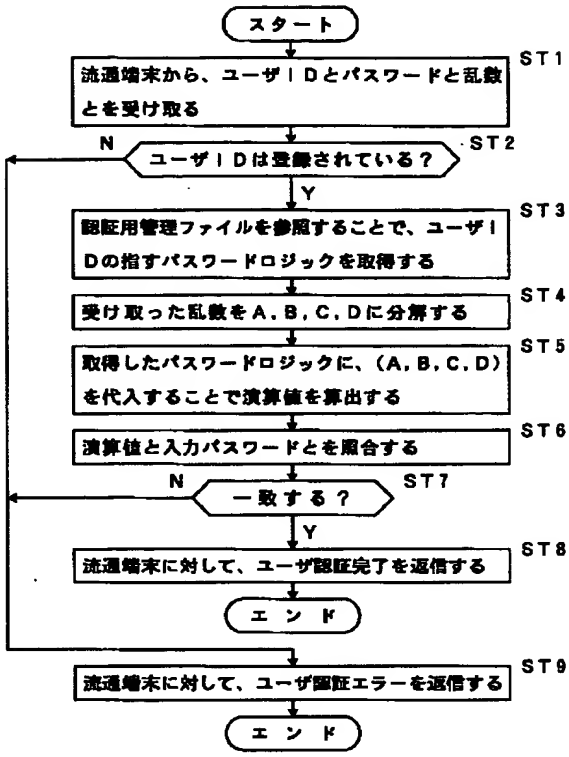
【図１７】

対話プログラムの処理フロー



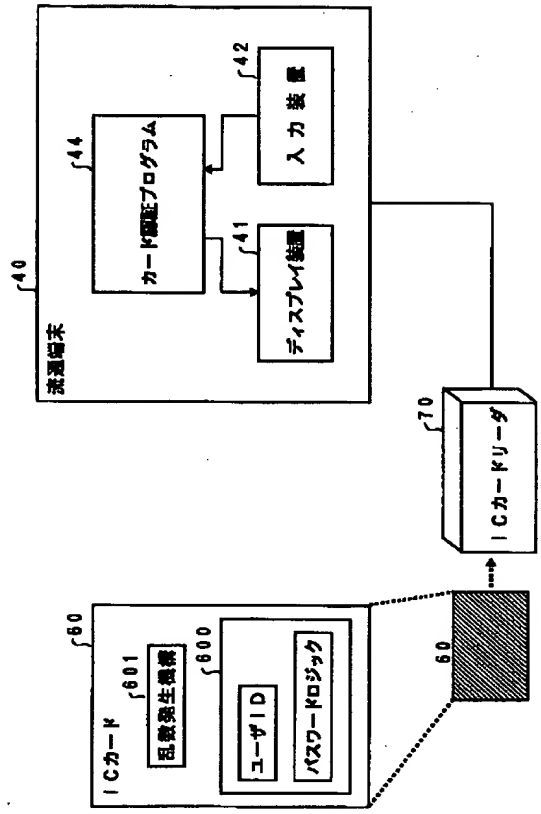
【図１８】

認証プログラムの処理フロー



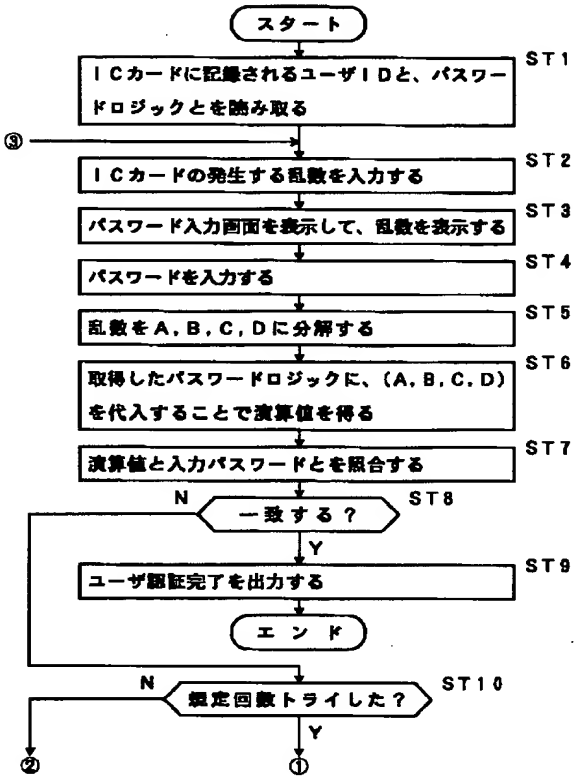
【図１９】

本発明の一実施例



【図２０】

カード認証プログラムの処理フロー



フロントページの続き

Ｆターム(参考)　5B049 AA05 BB11 CC39 DD01 DD04
EE23
5B085 AE03 AE08 AE12 AE15